

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-010930

(43)Date of publication of application : 14.01.2000

(51)Int.Cl.

G06F 15/00

G06F 13/00

G09C 1/00

H04L 9/32

(21)Application number : 10-177017

(71)Applicant : HITACHI LTD

(22)Date of filing : 24.06.1998

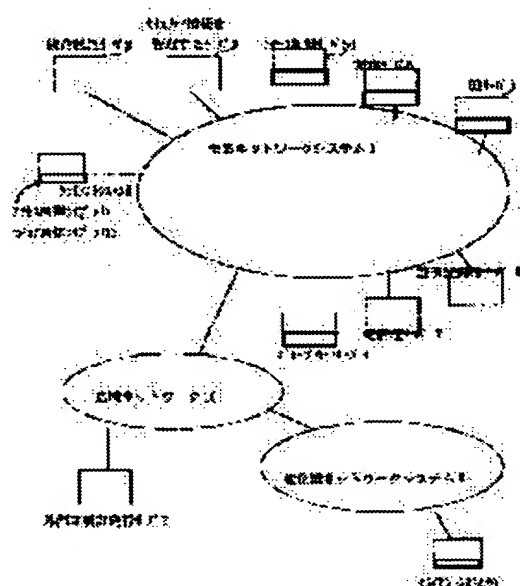
(72)Inventor : SAITO YOKO

## (54) ACCESS CONTROL METHOD FOR NETWORK SYSTEM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To attain a more flexible operation of a network by performing integrated and unitary management via an access control server for the access control processes which are so far carried out by a work server, a DB server, a groupware server, etc., in a conventional ACL and also grasping the temporary constraint set for the use of a network system and the user access state by means of the access tickets.

**SOLUTION:** An access control server 50 checks the access authority of a user to a work server 6 based on the confirmation result of the user's certificate acquired by an integrated authentication server 2 after the user is authenticated or when the work requests of the user are transferred to the server 50 from the clients 8 and 20. If the access authority of the user is legal, the work requests of the user are permitted to the server 6. In this case, a fact that the communication contents are never shown to the outsiders is guaranteed.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

**THIS PAGE BLANK (USPTO)**

[Date of extinction of right]

**THIS PAGE BLANK (USPTO)**

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-10930

(P2000-10930A)

(43) 公開日 平成12年1月14日 (2000.1.14)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 D 5 B 0 8 5
13/00	3 5 1	13/00	3 5 1 Z 5 B 0 8 9
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 E 5 K 0 1 3
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 B
			6 7 5 D

審査請求 未請求 請求項の数 3 O L (全 10 頁)

(21) 出願番号 特願平10-177017

(22) 出願日 平成10年6月24日 (1998. 6. 24)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72) 発明者 齊藤 洋子

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(74) 代理人 100077274

弁理士 磯村 雅俊 (外 1 名)

Fターム (参考) 5B085 AE02 AE06 AE10 AE23

5B089 AA21 AA22 AC05 AE08 AE09

AF00 CB02 CB03 CE00 DD03

DD07 EA03

5K013 AA08 FA01 GA05

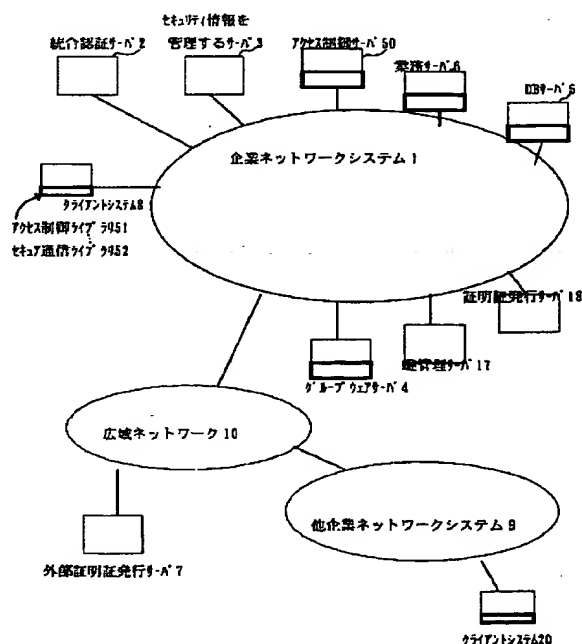
(54) 【発明の名称】 ネットワークシステムでのアクセス制御方法

## (57) 【要約】

【課題】 業務サーバ、DBサーバ、グループウェアサーバ等が従来のACLで行っていたアクセス制御処理を、アクセス制御サーバで集中的に一元管理する。またアクセスチケットを利用して、ネットワークシステム利用の一時的制約やユーザのアクセス状況を把握して、より柔軟なネットワーク運用を行う。

【解決手段】 ユーザの認証後あるいはクライアント8, 20からアクセス制御サーバ50に対してユーザの業務要求が転送された時に、アクセス制御サーバ50が統合認証サーバ2によるユーザの証明証の確認結果からユーザの業務サーバ6へのアクセス権限のチェックを行い、正当であれば業務サーバ6へのユーザの業務要求を許可する。その場合、通信内容を第三者には見せないことを保証する。

ネットワークシステムの構成図



**【特許請求の範囲】**

【請求項1】 ユーザが共有するクライアント端末、該クライアントからアクセスされ、業務処理のために利用される業務サーバ、および該ユーザが各サーバにアクセスする権限を有するか否かを確認するアクセス制御サーバが、相互に通信可能なネットワークシステムでのアクセス制御方法において、

ユーザを認証した後、あるいは該ユーザが共有するクライアント端末から該アクセス制御サーバに対して該ユーザの業務要求が転送された時に、

該アクセス制御サーバが、該ユーザの証明証の確認結果から該ユーザの業務サーバへのアクセス権限をチェックするステップと、

該アクセス制御サーバは、該アクセス権限が正当であれば該業務サーバへのユーザの業務要求を許可するステップとを有することを特徴とするネットワークでのアクセス制御方法。

【請求項2】 ユーザが共有するクライアント端末にアクセス制御ライブラリを設け、ユーザが各サーバにアクセスする権限を有するか否かを確認するアクセス制御サーバのID、該ユーザのID、アクセス制御リスト、運用の制約条件、該アクセス制御サーバの署名情報等から構成されるアクセスチケット情報を利用して、ユーザのアクセス権限のチェックを行うネットワークシステムでのアクセス制御方法において、

該アクセス制御サーバで、前記アクセスチケット情報を作成し、該アクセスチケット情報を該アクセス制御ライブラリに送信するステップと、

該アクセス制御ライブラリで、該アクセスチケット情報を用いて該ユーザの業務サーバへのアクセス権限チェックを行い、該業務サーバへのアクセス要求が適切であった場合には、該業務サーバに該ユーザの業務要求と該アクセスチケット情報を転送するステップと、

該業務サーバで、該ユーザによるデータへのアクセス権限のチェック結果を含むアクセス履歴情報を作成し、該ユーザによるアクセスの終了時に、業務結果と前記アクセス履歴情報を付加したアクセスチケット情報を該アクセス制御ライブラリに送信するステップと、

該アクセス制御ライブラリで、該アクセスチケット情報の内容を確認し、該ユーザのアクセス状況をチェックし、該アクセス状況に問題があった場合には、セキュリティ侵害情報を作成して、該セキュリティ侵害情報を付加したアクセスチケット情報を該アクセス制御サーバに送信するステップとを有することを特徴とするネットワークシステムでのアクセス制御方法。

【請求項3】 請求項1または2に記載のネットワークシステムでのアクセス制御方法において、

前記アクセス制御サーバ、クライアント端末のアクセス制御ライブラリ、及び業務サーバとの間でアクセスチケット情報を送受信する際に、通信の当事者以外には該ア

クセチケット情報の内容を見せないよう保証することとを特徴とするネットワークシステムでのアクセス制御方法。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明は、認証サーバ、アクセス制御サーバ、およびクライアントに対して、証明証を利用して広域ネットワークシステムでユーザ認証およびアクセス制御を行うネットワークシステムでのアクセス制御方法に関する。

**【0002】**

【従来の技術】インターネットの普及に伴いセキュリティをめぐる市場動向はめざましく変化してきた。特に、インターネットとイントラネットを統合する認証サーバは重要であり、広域ネットワークシステムでユーザを一元管理し、さらに集中的にアクセス制御を行う機能が求められている。ユーザ認証及びアクセス制御に証明証を利用する方法は、今後の広域ネットワークシステムでは一般的になると思われる。しかし、現実のネットワークシステムを考えると、最初から一元的なユーザ管理を行うことは困難であり、従来のユーザのネットワークシステムや業務形態に応じて、各業務サーバが個別にユーザのアクセス制御を行うことになると考えられる。このようなシステムの問題点としては、例えば企業内の人事移動に伴う職制変更等の時などに、複数の業務システムのデータベースのユーザ情報（例えば、認証情報やアクセス制御情報）を変更しなければならない点である。

【0003】本出願人は、本願より先に2つの提案（特願平9-76954号（先願A）、および特願平9-173532号（先願B）の各明細書および図面参照）を行っているが、先願Aでは、統合認証サーバで証明証によりユーザを認証することにより、従来のパスワードによる認証処理とのシングルサインオンを実現している。また、クライアントと統合認証サーバの双方でユーザに関するアクセス履歴を取得し、両者を比較することによりユーザの不正なアクセス状況をチェックしている。一方、先願Bでは、このセキュリティ管理モデルを拡張し、ユーザが複数の証明書により取り引きを行う場合に証明書の管理を容易化している。具体的には、統合認証サーバで1枚の統合証明書によりユーザを認証し、クライアントから業務APあるいは通信相手への通信要求に応じて、取り引きに必要な証明書を通信の当事者に送信するようにしている。先願Bの方式は、統合認証サーバで統合証明書の確認を集中的に行うシステム形態を想定しており、この場合には前記通信要求に関するユーザのアクセス権限の確認を統合証明書の認証処理の延長で行うことができる。なお、本願では、先願Aに合わせて認証サーバが発行する証明を証明証と記載する。

**【0004】**

【発明が解決しようとする課題】前述のように、統合認

証サーバで統合証明証の確認を集中的に行うシステム形態のアクセス制御方式については、先願Bに開示されている。しかしながら、認証処理のために統合認証サーバを設けず、通信の当事者間で、例えばセキュア通信ライブラリを実装することにより認証プロトコルに基づいて相互認証するシステム形態を考えると、アクセス制御を集中的に管理するアクセス制御サーバを設けたセキュリティ管理の方が適していると考ええる。

【0005】そこで、本発明の目的は、このような従来の課題を解決し、前記セキュア通信ライブラリと連携してアクセス制御を実現することにより、企業内のネットワークシステムを1箇所から集中管理することが可能なネットワークシステムでのアクセス制御方法を提供することにある。また、本発明の他の目的は、アクセス制御ライブラリを通信の当事者に実装したシステム形態を考慮し、その場合に必要となる前記アクセス制御サーバとの間のアクセス権限情報を送受信することができる機能を有するネットワークシステムでのアクセス制御方法を提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するため、本発明によるネットワークシステムでのアクセス制御方法では、①ユーザを認証した後に、あるいは該ユーザが共有するクライアントからアクセス制御サーバに対してユーザの業務要求が転送された時に、アクセス制御サーバが該ユーザの証明証の確認結果からユーザの該業務サーバへのアクセス権限のチェックを行い、正当であれば業務サーバへのユーザの業務要求を許可することの特徴とする。また、本発明のアクセス制御方法では、②クライアントにアクセス制御ライブラリを設ける場合には、アクセス制御サーバID、ユーザID、アクセス制御リスト、制約条件、署名情報等から構成されるアクセスチケット情報を利用して、ユーザのアクセス権限をチェックするために、次の処理を行うことも特徴とする。

(1)アクセス制御ライブラリで、前記アクセスチケットを用いて該ユーザの業務サーバへのアクセス権限チェックするステップと、該業務サーバへのアクセス要求が適切であった場合には該業務サーバに該ユーザの業務要求と前記アクセスチケットを転送するステップと、(2)業務サーバで、該ユーザによるデータへのアクセス権限のチェック結果を含むアクセス履歴情報を作成するステップと、該ユーザによるアクセスの終了時に業務結果と前記アクセス履歴情報を付加したアクセスチケットを該アクセス制御ライブラリに送信するステップと、(3)該アクセス制御ライブラリで、前記アクセスチケットの内容を確認して該ユーザのアクセス状況をチェックするステップと、該アクセス状況に問題があった場合にはセキュリティ侵害情報を作成するステップと、前記セキュリティ侵害を付加したアクセスチケットを該アクセス制御サーバに送信するステップとを有することである。

【0007】さらに、本発明のアクセス制御方法では、③アクセス制御サーバ、クライアントのアクセス制御ライブラリ及び業務サーバとの間で送受信されるアクセスチケットの情報については、通信の当事者以外には見せないことを保証することも特徴とする。本発明では、証明証を基にユーザのアクセス制御情報を参照することにより、全てのサーバへのアクセス制御を行う方式を提案する。すなわち、証明証を利用して広域ネットワークシステムでユーザ認証及びアクセス制御を行う認証サーバとアクセス制御サーバに関わるものであり、先願Aで提案した統合認証サーバとの連携を実現するアクセス制御方法を対象としている。これにより、業務サーバやデータベース(DB)サーバ、グループウェアサーバ等が、従来ではACL(アクセス制御リスト)で行っていたアクセス制御処理を、アクセス制御サーバで集中的に一元管理することができ、またアクセスチケットを利用することにより、ネットワークシステム利用の一時的制約やユーザのアクセス状況を把握することができ、柔軟なネットワークの運用が可能になる。

【0008】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図1は、本発明が適用されるネットワークシステムの構成図である。インターネットのような広域ネットワーク10には、企業ネットワークシステム1と他企業ネットワークシステム9が接続される。企業ネットワークシステム1には、複数のクライアント8(ここでは、1個のみ示されている)の他に、統合認証サーバ2、セキュリティ情報を管理するサーバ3、アクセス制御サーバ50、業務サーバ6、DBサーバ5、グループウェアサーバ4、鍵管理サーバ17、および証明証発行サーバ18等の各サーバが接続される。ここで、DBサーバ5および業務サーバ6は、クライアント8からアクセスされ、かつ業務処理のために利用されるサーバである。また、グループウェアサーバ4は、クライアント8へ最初の業務メニュー画面を送ったり、クライアント8の電子メールの送受信管理をしたり、ユーザのスケジュールを管理したりするサーバである。一方、他企業ネットワークシステム9には、クライアント20が接続されており、クライアント8のユーザとクライアント20は、電子取り引き等の特定の業務を証明証を用いて行うものとする。なお、クライアントシステム8には、アクセス制御ライブラリ51とセキュア通信ライブラリ52が備えられ、これを黒枠で示しており、ネットワークシステム1、9に接続されているクライアントシステム20と各サーバ4、5、6、50にも同じライブラリが備えられていることを黒枠で示している。

【0009】セキュリティ情報を管理するサーバ3は、DBサーバ5および業務サーバ6または他企業ネットワークシステム9へのアクセスを制御する情報と、業務に応じた証明証の情報を含むユーザの認証情報からなるセ

セキュリティ情報とを、一元的に管理するサーバである。公開鍵等もこのサーバ3で扱われる。また、統合認証サーバ2は、クライアント8から送られる証明証を確認し、サーバ3からセキュリティ情報を取得してユーザが企業ネットワークシステム1にログインする資格を持つか否かを調べる。このユーザの識別と認証処理が終了すると、ユーザのDBサーバ5および業務サーバ6または他企業ネットワークシステム9へのアクセス権限をチェックする必要があるため、該ユーザのACL（アクセス制御リスト）をサーバ3に要求する。該ACLの要求処理は、統合認証サーバ2がユーザの認証処理の延長で行うことにより、サーバ3から取得したセキュリティ情報の中からACLだけをアクセス制御サーバ50に渡すように実装することも可能であり、また、アクセス制御サーバ50が直接前記サーバ3からACLを取得するように実装することも可能である。また、ACLを取得するタイミングとしては、ユーザの認証処理の後でも、ユーザからの業務要求を受けた時でもよい。

【0010】図2は、本発明におけるACLを取得する手順および業務要求に対して許可／拒絶を受ける手順を示すシーケンスチャートである。図2(a)のシーケンスチャートでは、セキュア通信ライブラリ52がユーザを認証した後に、アクセス制御サーバ50にユーザのアクセス無限の確認要求を行い、アクセス制御サーバ50がサーバ3にACLを要求する処理例を示している。また、図2(b)のシーケンスチャートでは、クライアント8のユーザの業務要求がアクセス制御サーバ50に転送された時に、同時にユーザのアクセス権限の確認要求が行われ、アクセス制御サーバ50で該ユーザの証明証の確認結果からユーザの該業務サーバへのアクセス権限のチェックを行っている。いずれにしても、アクセス制御サーバ50は、サーバ3から取得したACL情報を用いて、ユーザがDBサーバ5および業務サーバ6または他企業ネットワークシステム9にアクセスする権限を持つかどうかを確認するサーバである。また、鍵管理サーバ17は、企業ネットワークシステム1内での暗号化通信で使用する通信当事者の鍵（秘密鍵と公開鍵の対）を生成するサーバである。広域ネットワーク10には、外部証明書発行サーバ7が接続されている。この外部証明書発行サーバ7は、所定の手順に従って外部証明書を発行するサーバである。例えば、クライアントシステム8とクライアントシステム20が広域ネットワーク10を介して取引を行う場合には、証明証発行サーバ18あるいは外部証明証発行サーバ7のいずれかに証明証あるいは外部証明証の発行を申請すればよい。

【0011】なお、ディレクトリサーバ（図示省略：各アプリケーションの存在場所を管理するサーバ）と呼ばれるサーバを配置して、ここにサーバ3の情報を有していても良い。この場合、クライアント8および各種サーバは、パソコン、ワークステーションを含む情報処理装

置である。さらに、クライアント8および各種サーバによって各々読み取り可能な記憶媒体上に実体化されたコンピュータプログラムを実行して、以下に記述するクライアント8および各種サーバの処理を行うことができる。例えば、アクセス制御ライブラリ51は、クライアント8上のコンピュータプログラムであり、アクセス制御サーバ50や業務サーバ6などと通信することにより、ユーザのアクセス状況を監視する。また、セキュア通信ライブラリ52は、クライアント8上や各種サーバ上のコンピュータプログラムであり、ネットワークシステム内の通信をセキュアに保護するために、通信当事者の相互認証、通信データの暗号化と内容の保証を行う。クライアント8または他企業ネットワークシステム9に接続されるクライアント20から証明証の情報を入力して、例えばDBサーバ5にログインすると、統合認証サーバ2が証明証の確認を行うが、この証明証を用いた具体的な認証処理シーケンスやシングルサインオンの実現方法については、前述の先願発明Aを参照すれば明らかとなる。

【0012】図2(a)には、ユーザがクライアント8からログイン後にセキュア通信ライブラリ52、アクセス制御ライブラリ51、アクセス制御サーバ50およびサーバ3間でやり取りする処理シーケンスが示されている。ユーザ11は、クライアント8の表示するユーザ認証画面(11a)にICカード内の証明証30の情報を入力することにより(11b)、企業ネットワークシステム1にログインする。ユーザの認証処理については、通信する双方のセキュア通信ライブラリ52がICカード内のユーザ11の証明証30の情報を確認し、乱数情報を送受信するチャレンジレスポンスシーケンスにより相互を認証しあい、そのセッションで利用する暗号鍵をネゴシエーションする処理を行うが、本発明では詳細の説明は省略する。具体的な認証シーケンスについては、先願発明Bを参照することで明らかとなる。証明証30の情報を利用してセキュア通信ライブラリ52の処理によりユーザ11の正当性が認められた後は、クライアント8上のアクセス制御ライブラリ51が証明証30の情報をを用いて、ユーザ11のアクセス権限を確認する。図2(a)に示すように、アクセス制御ライブラリ52は、アクセス制御サーバ50に対して証明証30の情報を送信する(11c)。これにより、アクセス制御サーバ50は、証明証30の情報を基にサーバ3に格納されているユーザ11のアクセス制御リスト(ACL)70を入手要求する(11d、11e)。

【0013】例えば、サーバ3がLDAP(Lightweight Data Access Protocol)に基づくディレクトリサーバである場合には、アクセス制御サーバ50はLDAPのプロトコルに基づきサーバ3に情報の問合せを行う。LDAPのプロトコル処理の一例については、先願発明Aを参照すれば明らかとなる。そして、ACL70の内容を



確認することにより、アクセス制御サーバ50は、ユーザ11の企業ネットワークシステム1へのアクセス権限が確認できる。具体的には、アクセス制御サーバ50から送信されてきたACL70の情報をもとに、クライアント8側のアクセス制御ライブラリ51がユーザ11向けの初期選択画面を表示し(11g)、以降、ユーザ11への業務処理サービスを行う(11h)。なお、アクセス制御サーバ50とアクセス制御ライブラリ51との間の通信はセキュア通信ライブラリ52の機能により保護されているため、相互で正しく認証され、情報が盗まれたり改ざんされたりする心配はない。該セキュア通信ライブラリ52の処理内容については、先願発明Aを参照されたい。

【0014】一方、図2(b)では、クライアント8のユーザの業務要求がアクセス制御サーバ50に転送された時に、アクセス制御サーバ50で該ユーザの証明証の確認結果からユーザの該業務サーバへのアクセス権限のチェックを行っている。例えば、EC向けアプリケーションのように、商品の購入時に初めて認証処理を行う時等に相当する。クライアント8から業務要求を受けた時に(10a)、セキュア通信ライブラリ52はユーザ認証画面を表示し(10b)、ユーザはユーザ認証画面にICカード内の証明証30の情報を入力する(10c)。証明証30の情報を利用してセキュア通信ライブラリ52の処理によりユーザ11の正当性が認められた後は、クライアント8上のアクセス制御ライブラリ51が証明証30の情報をを用いて、ユーザ11のアクセス権限を確認する。図2(b)に示すように、アクセス制御ライブラリ52は、アクセス制御サーバ50に対して証明証30の情報を送信する(10d)。その結果、アクセス制御サーバ50は証明証30の情報を基に、サーバ3に格納されているユーザ11のアクセス制御リスト(ACL)70を入手要求する(10e)。そして、ACL70の内容を確認することにより(ACL70e)、アクセス制御サーバ50は、ユーザ11の企業ネットワークシステム1へのアクセス権限が確認できる。具体的には、アクセス制御サーバ50から送信されてきたACL70の情報(ACL70f)を基に、クライアント8側のアクセス制御ライブラリ51がユーザ11の業務要求の許可あるいは拒絶を応答する(10g)。

【0015】図3は、本発明に用いられるACL形式の情報例を示す図である。ACLには種々の形式が考えられるが、ユーザ情報の更新時に修正作業を最小限にするために、図3(a)に示すようにユーザ情報71とユーザ権限情報72、およびアクセス関連情報73をツリー構造の別データとして管理している。ユーザ情報71には、図3(b)に示すように企業内ネットワーク1内で当ユーザを一意的に識別するために付与されているユーザ識別名称と証明証の情報の対応が管理されている。このユーザ識別名称については、企業システムの名称ポリ

シーの規定に従う。また、図3(c)に示すようにユーザに関するその他の情報(例えば住所、家族構成や入社年度等の情報)も必要に応じて参照できるようになっている。ユーザ権限情報72には、図3(d)に示すようにユーザとユーザの権限の対応が管理されている。例えばユーザをA0、A1、A2、A3という権限クラスで分類してアクセスさせるようなシステムの場合は、事例1に示すようにユーザごとに権限クラスを指定しておく。また、このようなクラスの代りに、事例2(図3(e))に示すように所属や職位からなる職制情報を利用してよい。

【0016】これらの権限クラスや職制情報に対応させて、どのような権限を許可するかを規定しておくのが、図3(f)に示すようなアクセス関連情報73である。アクセス関連情報73には、企業ネットワークシステム1内の全リソースに関するアクセス権限情報が定義されているので、例えば、図3(f)に示すように、クラスA1のユーザ11についての企業ネットワークシステム1内のアクセス権限が、DBサーバ5のファイル501に対する参照と更新、ファイル502に対する参照が許可され、業務サーバ6のAP601の起動が許可されていることがわかる。また、接続形態の条件として、企業ネットワーク内からのアクセスだけが許可されており、リモートアクセスによる接続は許可されていないことがわかる。このようにして、全てのユーザに対するアクセス制御情報を一元管理するが、よりきめ細かなアクセス制御、例えばファイル503のレコード5031(いずれも図示省略)をユーザ11だけに見せるというアクセスを制御したい場合には、DBサーバ5内のアクセス制御機能を利用することも可能である。職制変更時のユーザ情報変更作業を考えると、例えば、ユーザ11の担当業務が変更になった場合には、図3(e)に示すユーザ権限情報72を変更すればよく、ユーザ11のアカウントが削除される場合には、図3(b)～(e)に示すユーザ情報71とユーザ権限情報72からユーザ11の項目を削除すればよい。従来方式において、業務サーバ毎にユーザのACLを管理していたシステム形態では、ユーザ情報の修正が業務サーバ毎に必要であったことを考えると、本発明では、ユーザ情報を一個所で変更できる点に利点がある。

【0017】図4は、本発明におけるアクセスチケットを用いた制御手順を示すシーケンスチャートである。アクセス制御サーバ50がアクセスチケット75を用いて、さらにきめ細かな運用を考慮したアクセス制御を行う事例について説明する。図4に示すように、セキュア通信ライブラリ52はユーザ認証画面を表示し(14a)、ユーザはユーザ認証画面にICカード内の証明証31の情報を入力する(14b)。証明証31の情報を利用してセキュア通信ライブラリ52の処理によりユーザ14の正当性が認められた後は、クライアント20上

のアクセス制御ライブラリ51が証明証31の情報を用いて、ユーザ14のアクセス権限を確認する。次に、アクセス制御サーバ50に対してユーザ14のアクセス権限の確認要求を行うと(14c)、アクセス制御サーバ50は業務サーバ6にACLを要求する(14d)。このように、ユーザ14がクライアント20からネットワークシステム1にログインする場合、アクセスチケット75aの中に9時から17時までという一時的な運用の制約条件76をつけることが可能である。この場合、アクセス制御サーバ50は、クライアント20側のアクセス制御ライブラリ51に、アクセス制御サーバID、ユーザ14のユーザ識別名、ユーザ14のACL、制約条件76、およびアクセス制御サーバ50の署名情報から構成されるアクセスチケット75aを作成し、アクセス制御ライブラリ51に送信する(75a)。アクセス制御サーバ50とアクセス制御ライブラリ51との間の通信はセキュア通信ライブラリ52の機能により保護されているため、相互で正しく認証され、情報が盗まれたり改ざんされる心配はない。また、セキュア通信ライブラリ51は、アクセスチケット75aの内容が確かにアクセス制御サーバ50によって作成されたものであることを保証するために、署名情報を付加している。

【0018】次に、図4において、アクセス制御ライブラリ51がアクセスチケット75aを受け取ると、クライアント20上のグループウェアアプリケーションはユーザ14に対して初期選択画面を表示する(14e)。この初期選択画面は、ユーザ14のACLに基づき作成されるもので、ユーザ14に権限に許されている業務だけが表示される。また、ユーザ14が表示された以外の業務のアプリケーションを起動するとユーザ14に対して警告を発し、アクセス履歴情報12が取得される。ユーザ14が前記初期選択画面の中の業務の中から業務サーバ6のAP60(図示省略)を起動した場合(14f)、ユーザ14によるAP601(図示省略)の業務要求は、アクセス制御ライブラリ51から業務サーバ6に転送されるが(75d)、その時に前記アクセスチケット75aも添付される。業務サーバ6は、このアクセスチケット75aの内容を確認することにより、以降の業務処理AP601を実行する。具体的には、ACLと制約条件76を考慮した処理を行うので、図4に示すACLに許可された以外のAP601の修正や業務AP602の起動等は許さず、時刻が17時を過ぎたならばユーザ14に対する処理を打ち切る。そして、業務サーバ6は、ユーザ14のアクセス状況についてはアクセス履歴情報12に記録しておく。

【0019】業務が終了すると、業務サーバ6は、業務サーバID、ユーザ14のユーザ識別名、ユーザ14によるアクセス履歴情報12、および業務サーバ6の署名情報から構成されるアクセスチケット75bを作成し、アクセス制御ライブラリ51に送信する(75b)。な

お、業務サーバ6とアクセス制御ライブラリ51との間の通信はセキュア通信ライブラリ52の機能により保護されているため、相互で正しく認証され、情報が盗まれたり改ざんされたりする心配はない。アクセス制御ライブラリ51は、ユーザ14に業務結果を出力するとともに(14g)、業務サーバ6から受信したアクセスチケット75bのアクセス履歴情報12を確認し、ユーザ14のアクセスに問題があるかどうかをチェックし、セキュリティ上の問題を発見した場合には、セキュリティ侵害情報13とアクセス制御ライブラリ51の署名情報を作成してアクセスチケット75cに付加して送信することにより(75c)、アクセス制御サーバ50に報告する。また、図4の例では、制約条件76をアクセス制御サーバ50が付加したが、例えば、ユーザのICカードの中にオペレーション情報を格納しておき、その情報を図4のアクセス制御ライブラリ51によるユーザ14のアクセス権限の確認要求の時にアクセス制御サーバ50に送るような実装も可能である。

【0020】

【発明の効果】以上述べたように、本発明によれば、業務サーバ、DBサーバ、あるいはグループウェアサーバ等が従来のACLで行っていたアクセス制御処理を、アクセス制御サーバにより一元管理できるので、企業内ネットワークシステムを一個所から集中管理することが可能である。また、アクセスチケットを利用することにより、ネットワークシステム利用の一時的制約やユーザのアクセス状況を把握できるので、より柔軟なネットワーク運用が可能となる。さらに、前記アクセスチケットの情報は、クライアント、業務サーバ、アクセス制御サーバの間でセキュアに送受信されるため、悪意のある第三者が盗聴して悪用することは不可能となる。

【図面の簡単な説明】

【図1】本発明が適用されるネットワークシステムの構成図である。

【図2】本発明におけるACL問い合わせ手順および業務要求手順の各シーケンスチャートである。

【図3】本発明で用いられるACL形式の情報例を示す図である。

【図4】本発明におけるアクセスチケットを用いた制御手順のシーケンスチャートである。

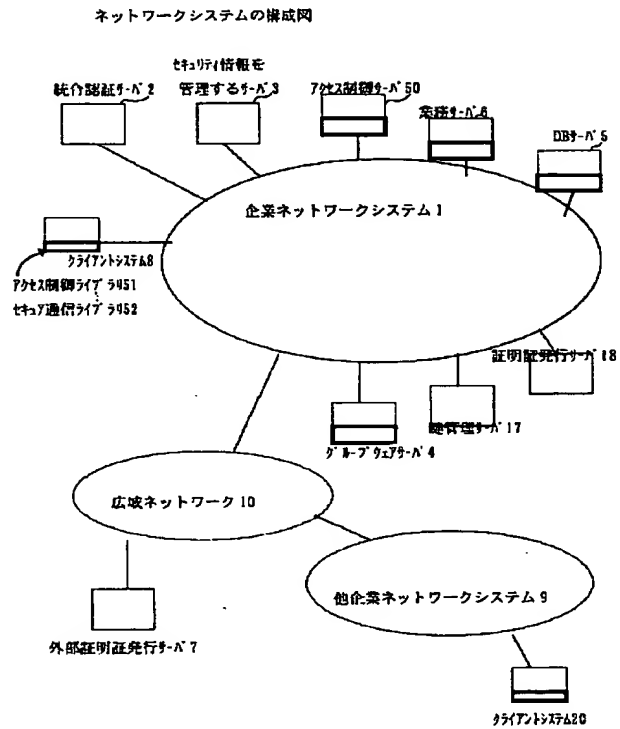
【符号の説明】

1…企業ネットワークシステム、2…統合認証サーバ、3…セキュリティ情報を管理するサーバ、4…グループウェアサーバ、5…DBサーバ、6…業務サーバ、7…外部証明証発行サーバ、8、20…クライアントシステム、9…他企業のネットワークシステム、10…広域ネットワークシステム、11、14…ユーザ、12…アクセス履歴情報、13…セキュリティ侵害情報、17…鍵管理サーバ、18…証明証発行サーバ、30、31…証明証、70…ACL(アクセス制御リスト)、75…ア

クセステケット、76…制約条件、51…アクセス制御ライブラリ、52…セキュア通信ライブラリ、71…ユーザ情報、72…ユーザ権限情報、73…アクセス関連

情報、50…アクセス制御サーバ、A0～A3…権限クラス。

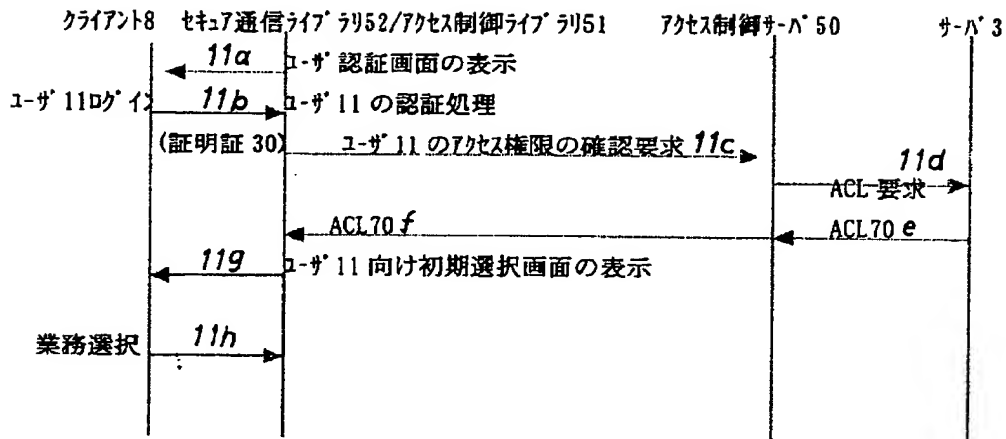
【図1】



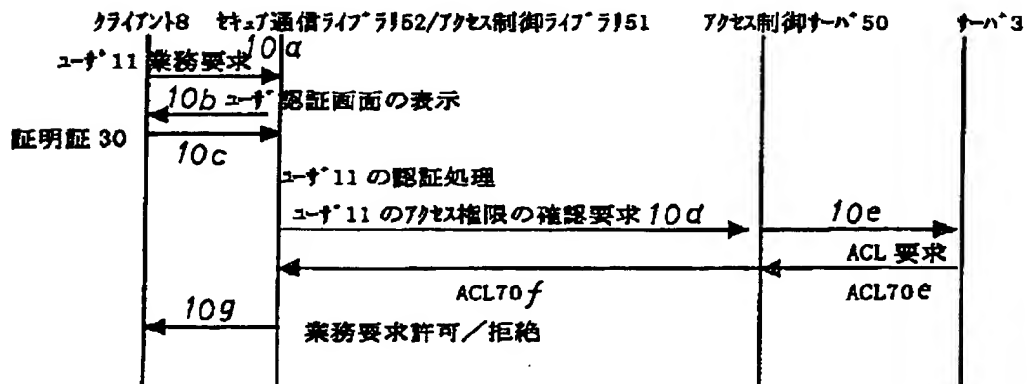
【図2】

## ACL問合せ手順

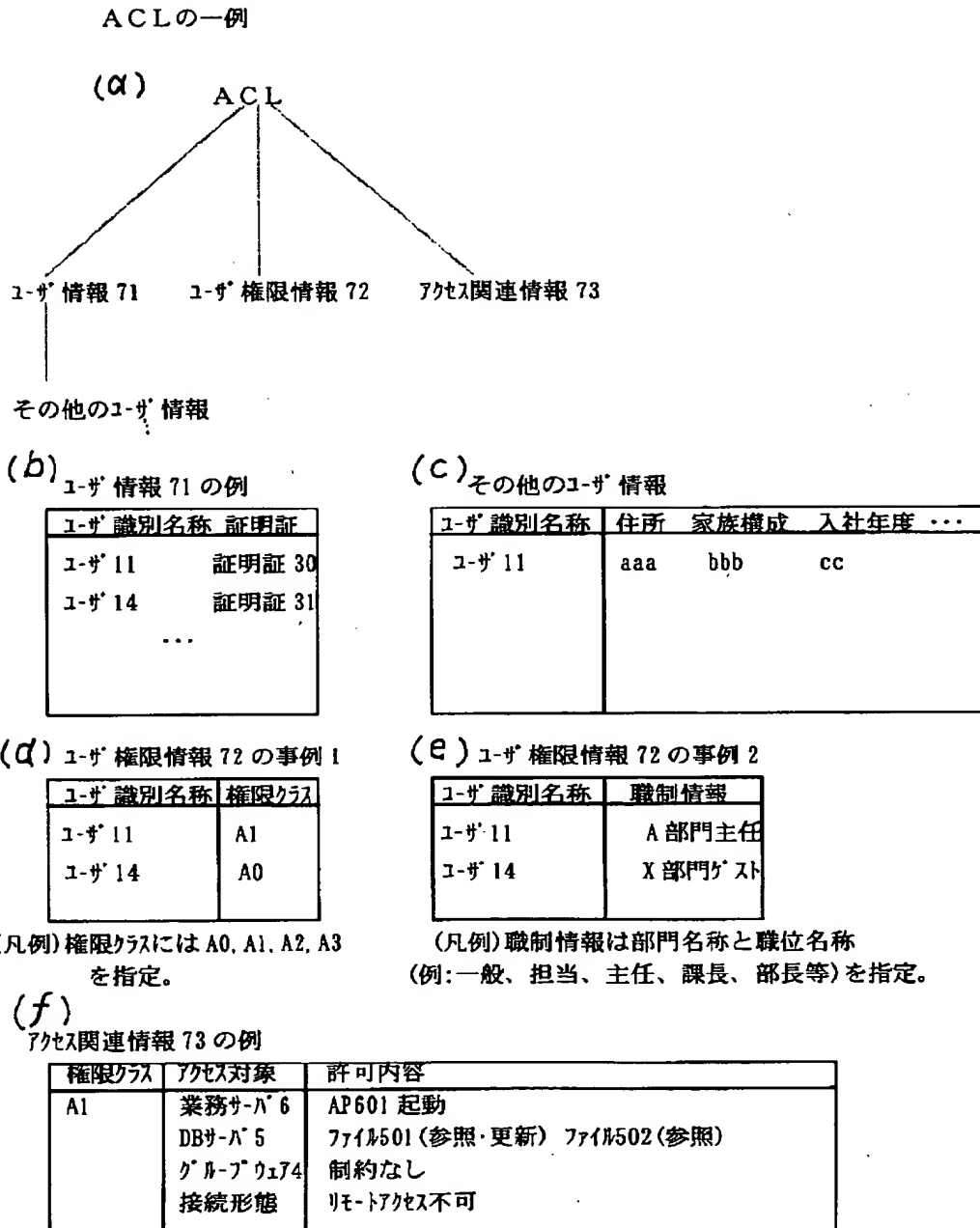
(a)



(b)



【図3】



【図4】

## アクセスチケットを用いた制御手順

